

A New Quantum Data Processing Inequality

Salman Beigi

School of Mathematics, Institute for Research in Fundamental Sciences (IPM)

P.O. Box 19395-5746, Tehran, Iran

Abstract

Quantum data processing inequality bounds the set of bipartite states that can be generated by two far apart parties under local operations; Having access to a bipartite state as a resource, two parties cannot locally transform it to another bipartite state with a mutual information greater than that of the resource state. But due to the additivity of quantum mutual information under tensor product, data processing inequality gives no bound when the parties are provided with infinitely many copies of the resource state. In this paper we introduce a measure of correlation on bipartite quantum states that is not additive and gives the same number when computed for multiple copies. Then by proving a data processing inequality for this measure, we find a bound on the set of states that can be generated under local operations even when an infinite number of copies of the resource state is available. We show that this measure fully characterizes bipartite states from which common randomness can be distilled under local operations.

1 Introduction

Let ρ_{AB} be a bipartite quantum state on registers A and B , and assume that infinitely many copies of ρ_{AB} are shared between two parties Alice and Bob. The goal of Alice and Bob is to generate some bipartite state σ_{EF} under local operations but without communication. That is for some n , they want to apply local super-operators $\Phi_{A^n \rightarrow E}$ and $\Psi_{B^n \rightarrow F}$ such that

$$\Phi \otimes \Psi(\rho_{AB}^{\otimes n}) = \sigma_{EF}.$$

Typical examples of this problem are entanglement distillation and common randomness distillation under local operations, in which case σ_{EF} is an ebit or one bit of shared randomness.

To answer this question one cannot look for such local operators by brute-force search since we assume n , the number of copies of the resource state ρ_{AB} is arbitrarily large. On the other hand to obtain some necessary conditions on the existence of Φ and Ψ one may compare the strength of correlations of $\rho_{AB}^{\otimes n}$ and σ_{EF} . If σ_{EF} has more correlation than $\rho_{AB}^{\otimes n}$, then such operations do not exist since local transformations do not generate correlation. Nevertheless again since n can be arbitrarily large, the standard measures of correlation provide us with no bound. For instance the data processing inequality of mutual information states that if $\rho_{AB}^{\otimes n}$ can be locally transformed to σ_{EF} then

$$nI(A; B)_\rho = I(A^n; B^n)_{\rho^{\otimes n}} \geq I(E; F)_\sigma, \quad (1)$$

where $I(\cdot, \cdot)$ denotes the quantum mutual information. This inequality is loose for sufficiently large n and gives us no bound if $I(A; B)_\rho \neq 0$.

In the classical case where ρ_{AB} and σ_{EF} are bipartite random variables, this problem is partially answered by Kang and Ulukus in [1] where (instead of mutual information) *maximal correlation* is used as a measure of correlation. The main useful properties of maximal correlation for this problem are that it is *not* additive on independent copies of a bipartite distribution, and that it satisfies some data processing inequality. Kamath and Anantharam [2] also consider this problem where they use “hypercontractivity ribbon” to find a bound. Interestingly they show that their approach gives a stronger bound comparing to maximal correlation.

The main contribution of this paper is to generalize maximal correlation to the quantum case.

2 A new measure of correlation

Let \mathcal{H}_A be the Hilbert space corresponding to register A , and denote the space of linear operators acting on \mathcal{H}_A by $\mathbf{L}(\mathcal{H}_A)$. Similarly define $\mathbf{L}(\mathcal{H}_B)$ and equip these two spaces with the Hilbert-Schmidt inner product, i.e., $\langle M, N \rangle = \text{tr}(M^\dagger N)$. This inner product induces a norm on the space of linear operators which we denote by $\|\cdot\|_2$.

For a bipartite quantum state ρ_{AB} define

$$\mu(\rho_{AB}) = \max |\text{tr}(\rho_{AB} X_A \otimes Y_B^\dagger)|$$

$$\text{tr}(\rho_A X_A) = \text{tr}(\rho_B Y_B) = 0, \quad (2)$$

$$\text{tr}(\rho_A X_A X_A^\dagger) = \text{tr}(\rho_B Y_B Y_B^\dagger) = 1. \quad (3)$$

Here ρ_A and ρ_B are the reduced density matrices on subsystems A and B respectively, and $X_A \in \mathbf{L}(\mathcal{H}_A)$ and $Y_B \in \mathbf{L}(\mathcal{H}_B)$.

To study properties of $\mu(\rho_{AB})$ let us define

$$\tilde{\rho}_{AB} = (I_A \otimes \rho_B^{-1/2}) \rho_{AB} (\rho_A^{-1/2} \otimes I_B),$$

where inverses of ρ_A and ρ_B are defined on their supports.

Theorem 1 $\mu(\rho_{AB})$ is equal to the second Schmidt coefficient of $\tilde{\rho}_{AB}$ as a vector in the tensor product Hilbert space $\mathbf{L}(\mathcal{H}_A) \otimes \mathbf{L}(\mathcal{H}_B)$.

Proof: Let $R_A = \rho_A^{1/2} X_A$ and $S_B = Y_B^\dagger \rho_B^{1/2}$. Using these changes of variables $\mu(\rho_{AB})$ is equivalently equal to

$$\mu(\rho_{AB}) = \max |\text{tr}(\tilde{\rho}_{AB} R_A \otimes S_B)|$$

$$\langle \rho_A^{1/2}, R_A \rangle = \langle \rho_B^{1/2}, S_B \rangle = 0, \quad (4)$$

$$\|R_A\|_2 = \|S_B\|_2 = 1. \quad (5)$$

Let

$$\tilde{\rho}_{AB} = \sum_i \lambda_i M_i \otimes N_i,$$

be the Schmidt decomposition of $\tilde{\rho}_{AB} \in \mathbf{L}(\mathcal{H}_A) \otimes \mathbf{L}(\mathcal{H}_B)$ where $\lambda_1 \geq \lambda_2 \geq \dots$ are the Schmidt coefficients and $\{M_i\}$ and $\{N_i\}$ are orthonormal bases for $\mathbf{L}(\mathcal{H}_A)$ and $\mathbf{L}(\mathcal{H}_B)$ respectively. Note that

$$\lambda_1 = \max_{\|V\|_2=\|W\|_2=1} \text{tr}(\tilde{\rho}_{AB} V_A \otimes W_B),$$

and using Cauchy-Schwarz inequality we have

$$\begin{aligned} \lambda_1 &= \text{tr}(M_1^\dagger \otimes N_1^\dagger \tilde{\rho}_{AB}) \\ &= \text{tr}\left[\left(\rho_A^{-1/2} M_1^\dagger\right) \otimes \left(N_1^\dagger \rho_B^{-1/2}\right) \rho_{AB}\right] \\ &= \text{tr}\left[\left(\rho_{AB}^{1/2} (\rho_A^{-1/2} M_1^\dagger \otimes I_B)\right) \left((I_A \otimes N_1^\dagger \rho_B^{-1/2}) \rho_{AB}^{1/2}\right)\right] \\ &\leq \left[\text{tr}\left(\rho_{AB} (\rho_A^{-1/2} M_1^\dagger M_1 \rho_A^{-1/2} \otimes I_B)\right)\right]^{1/2} \cdot \left[\text{tr}\left(\rho_{AB} (I_A \otimes \rho_B^{-1/2} N_1 N_1^\dagger \rho_B^{-1/2})\right)\right]^{1/2} \\ &= \left[\text{tr}\left(\rho_A (\rho_A^{-1/2} M_1^\dagger M_1 \rho_A^{-1/2})\right)\right]^{1/2} \cdot \left[\text{tr}\left(\rho_B (\rho_B^{-1/2} N_1 N_1^\dagger \rho_B^{-1/2})\right)\right]^{1/2} \\ &= \left[\text{tr}(M_1^\dagger M_1)\right]^{1/2} \cdot \left[\text{tr}(N_1 N_1^\dagger)\right]^{1/2} \\ &= 1. \end{aligned}$$

On the other hand observe that $\|\rho_A^{1/2}\|_2 = \|\rho_B^{1/2}\|_2 = 1$ and $|\text{tr}(\tilde{\rho}_{AB} \rho_A^{1/2} \otimes \rho_B^{1/2})| = |\text{tr}(\rho_{AB})| = 1$. As a result,

$$\lambda_1 = 1,$$

and we can take $M_1 = \rho_A^{1/2}$ and $N_1 = \rho_B^{1/2}$.

Now for R_A and S_B satisfying (4) and (5) we have

$$\begin{aligned}
|\text{tr}(\tilde{\rho}_{AB} R_A \otimes S_B)| &= \left| \sum_{i \geq 1} \lambda_i \langle R^\dagger, M_i \rangle \langle S^\dagger, N_i \rangle \right| \\
&= \left| \sum_{i \geq 2} \lambda_i \langle R^\dagger, M_i \rangle \langle S^\dagger, N_i \rangle \right| \\
&\leq \left(\sum_{i \geq 2} \lambda_i |\langle R^\dagger, M_i \rangle|^2 \right)^{1/2} \left(\sum_{i \geq 2} \lambda_i |\langle S^\dagger, N_i \rangle|^2 \right)^{1/2} \\
&\leq \lambda_2,
\end{aligned}$$

where in the last line we use $1 = \|R\|_2^2 = \sum_{i \geq 2} |\langle R^\dagger, M_i \rangle|^2$ and similarly $1 = \sum_{i \geq 2} |\langle S^\dagger, N_i \rangle|^2$. These inequalities are tight for $R = M_2^\dagger$ and $S = N_2^\dagger$. We conclude that $\mu(\rho_{AB}) = \lambda_2$. \square

Let us consider the special case where A and B are classical registers. If $\{|i\rangle : 1 \leq i \leq d_A\}$ and $\{|k\rangle : 1 \leq k \leq d_B\}$ are computational bases of \mathcal{H}_A and \mathcal{H}_B respectively, then ρ_{AB} is diagonal in the basis $\{|i\rangle|k\rangle : 1 \leq i \leq d_A, 1 \leq k \leq d_B\}$. Let us denote $p_{ik} = \langle i|k|\rho_{AB}|i\rangle|k\rangle$, so we can think of a joint distribution P_{AB} with marginals P_A and P_B . Then it is easy to see that

$$\begin{aligned}
\mu(P_{AB}) &= \max \mathbb{E}(f(i)g(k)) \\
\mathbb{E}(f(i)) &= \mathbb{E}(g(k)) = 0, \\
\mathbb{E}(f(i)^2) &= \mathbb{E}(g(k)^2) = 1,
\end{aligned}$$

where the maximum is taken over all real functions f and g defined on $\{1, \dots, d_A\}$ and $\{1, \dots, d_B\}$ respectively, and \mathbb{E} denotes the expectation value with respect to P_{AB} . This parameter $\mu(P_{AB})$ is first introduced by Hirschfeld [3] and is called the *Hirschfeld-Gebelein-Rényi maximal correlation* or simply the maximal correlation [3, 4, 5, 6]. It is not hard to see that $\mu(P_{AB})$ satisfies a data processing inequality. Moreover it is proved by Witsenhausen [7] that for $P_{AA'B'}$ where AB and $A'B'$ are independent we have

$$\mu(P_{AA'B'}) = \max\{\mu(P_{AB}), \mu(P_{A'B'})\}.$$

The maximal correlation can be reformulated using Theorem 1. Define

$$\tilde{p}_{ik} = p_i^{-1/2} p_k^{-1/2} p_{ik},$$

and let \tilde{P}_{AB} be a $d_A \times d_B$ matrix whose ik -th entry is \tilde{p}_{ik} . It is easy to see that Schmidt coefficients of \tilde{P}_{AB} are in one-to-one correspondence with singular values of \tilde{P}_{AB} . So in the classical case $\mu(P_{AB})$ is equal to the second singular value of \tilde{P}_{AB} . For example if P_{AB} denotes two perfectly correlated random variables, then \tilde{P}_{AB} is the identity matrix and $\mu(P_{AB}) = 1$. This latter formulation of maximal correlation is first found¹ by Kang and Ulukus [1].

See [8, 9] for some extensions and applications of the maximal correlation.

Theorem 2 $\mu(\cdot)$ satisfies the following properties:

- (a) $\mu(\rho_{AB} \otimes \sigma_{A'B'}) = \max\{\mu(\rho_{AB}), \mu(\sigma_{A'B'})\}$.
- (b) Let $\Phi_B : \mathbf{L}(\mathcal{H}_B) \rightarrow \mathbf{L}(\mathcal{H}_{B'})$ be a completely positive trace non-increasing super-operator. Let $\sigma_{AB'} = \alpha \mathcal{I}_A \otimes \Phi_B(\rho_{AB})$ where $\alpha \geq 1$ is an appropriate normalization factor. Then $\mu(\sigma_{AB'}) \leq \alpha^{1/2} \mu(\rho_{AB})$.

Proof: (a) Let $\lambda_1 = 1 \geq \lambda_2 \geq \dots$ and $\zeta_1 = 1 \geq \zeta_2 \geq \dots$ be the Schmidt coefficients of $\tilde{\rho}_{AB}$ and $\tilde{\sigma}_{A'B'}$ respectively. By Theorem 1, $\mu(\rho_{AB} \otimes \sigma_{A'B'})$ is equal to the second Schmidt coefficient of $\tilde{\rho}_{AB} \otimes \tilde{\sigma}_{A'B'}$ which is equal to

$$\max\{\lambda_1 \zeta_2, \zeta_1 \lambda_2\} = \max\{\lambda_2, \zeta_2\} = \max\{\mu(\rho_{AB}), \mu(\sigma_{A'B'})\}.$$

¹It is not mentioned in [1] that the second singular value of \tilde{P}_{AB} is equal to the maximal correlation of P_{AB} , but (for example) Theorem 1 shows this connection.

(b) If Φ_B were trace-preserving we could have used Stinespring's dilation. Local isometries obviously do not change $\mu(\rho_{AB})$ and we would have needed $\mu(\sigma_{AB}) \leq \mu(\sigma_{AA'B})$ which is easy to prove. Here we present a proof for the more general case where Φ_B is trace non-increasing.

Let X_A and $Y_{B'}$ be the optimizers for $\sigma_{AB'}$ satisfying (2) and (3). Let Φ^* be the adjoint of Φ , i.e., $\text{tr}(\Phi(M)N) = \text{tr}(M\Phi^*(N))$. Note that Φ^* is completely positive since Φ is completely positive, and $\Phi^*(I) \leq I$ because Φ is trace non-increasing. Define $Z = \alpha^{1/2}\Phi^*(Y)$. Observe that $\sigma_A = \rho_A$ and $\sigma_{B'} = \alpha\Phi(\rho_B)$. Thus $\text{tr}(\rho_A X) = \text{tr}(\sigma_A X) = 0$ and $\text{tr}(\rho_A X X^\dagger) = \text{tr}(\sigma_A X X^\dagger) = 1$. Moreover,

$$\text{tr}(\rho_B Z) = \alpha^{1/2}\text{tr}(\rho_B \Phi^*(Y)) = \alpha^{1/2}\text{tr}(\Phi(\rho_B)Y) = \alpha^{-1/2}\text{tr}(\sigma_B Y) = 0,$$

and

$$\begin{aligned} \text{tr}(\rho_{AB} X \otimes Z^\dagger) &= \alpha^{1/2}\text{tr}(\rho_{AB} X \otimes \Phi^*(Y^\dagger)) \\ &= \alpha^{1/2}\text{tr}(\mathcal{I}_A \otimes \Phi_B(\rho_{AB})X \otimes Y^\dagger) \\ &= \alpha^{-1/2}\text{tr}(\sigma_{AB'} X \otimes Y^\dagger) \\ &= \alpha^{-1/2}\mu(\sigma_{AB'}), \end{aligned}$$

where we use the fact that both Φ and Φ^* are hermitian-preserving. Therefore, we conclude that $\mu(\rho_{AB}) \geq \alpha^{-1/2}\mu(\sigma_{AB'})$ if $\text{tr}(\rho_B Z Z^\dagger) \leq 1$. To prove the latter, observe that

$$\begin{pmatrix} Y Y^\dagger & Y \\ Y^\dagger & I \end{pmatrix} = \begin{pmatrix} Y \\ I \end{pmatrix} \begin{pmatrix} Y^\dagger & I \end{pmatrix}$$

is positive semidefinite. Since Φ^* is *completely* positive,

$$\begin{pmatrix} \Phi^*(Y Y^\dagger) & \Phi^*(Y) \\ \Phi^*(Y^\dagger) & \Phi^*(I) \end{pmatrix},$$

is positive semidefinite. On the other hand $\Phi^*(I) \leq I$. Therefore,

$$\begin{pmatrix} \Phi^*(Y Y^\dagger) & \Phi^*(Y) \\ \Phi^*(Y^\dagger) & I \end{pmatrix},$$

is positive semidefinite as well. This means that $\Phi^*(Y Y^\dagger) \geq \Phi^*(Y)\Phi^*(Y^\dagger)$. Now using $\rho_B \geq 0$ we have

$$\begin{aligned} \text{tr}(\rho_B Z Z^\dagger) &= \alpha \text{tr}(\rho_B \Phi^*(Y)\Phi^*(Y^\dagger)) \\ &\leq \alpha \text{tr}(\rho_B \Phi^*(Y Y^\dagger)) \\ &= \alpha \text{tr}(\Phi(\rho_B) Y Y^\dagger) \\ &= \text{tr}(\sigma_B Y Y^\dagger) \\ &= 1. \end{aligned}$$

We are done. □

The following corollary is the main result of this paper and is a direct consequence of the above theorem.

Corollary 3 *Suppose that $\rho_{AB}^{\otimes n}$, for some n , can be locally transformed to σ_{EF} (under completely positive trace-preserving super-operators). Then*

$$\mu(\rho_{AB}) \geq \mu(\sigma_{EF}).$$

The following example reveals the strength of this corollary. Let $|\psi\rangle_{AB} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ be the Bell state on two qubits. Define

$$\rho_{AB}^{(p)} = (1-p)\frac{I_{AB}}{4} + p|\psi\rangle\langle\psi|_{AB},$$

where $0 \leq p \leq 1$ and $I_{AB}/4$ is the maximally mixed state. Note that $\rho_A^{(p)} = I_A/2$ and $\rho_B^{(p)} = I_B/2$ for every p . Therefore,

$$\begin{aligned}\mu(\rho_{AB}^{(p)}) &= \max \operatorname{tr}(\rho_{AB}^{(p)} X \otimes Y^\dagger) \\ &\quad \operatorname{tr}(X) = \operatorname{tr}(Y) = 0, \\ &\quad \operatorname{tr}(XX^\dagger) = \operatorname{tr}(YY^\dagger) = 2.\end{aligned}$$

For X and Y satisfying the above equations we have

$$\begin{aligned}|\operatorname{tr}(\rho_{AB}^{(p)} X \otimes Y^\dagger)| &= \left| \frac{1-p}{4} \operatorname{tr}(X \otimes Y^\dagger) + p \langle \psi | X \otimes Y^\dagger | \psi \rangle \right| \\ &= \frac{p}{2} |\operatorname{tr}(X^T Y^\dagger)| \\ &\leq \frac{p}{2} \|X\|_2 \cdot \|Y\|_2 \\ &= p.\end{aligned}$$

This upper bound is achievable at $X = Y = |0\rangle\langle 0| - |1\rangle\langle 1|$. Therefore,

$$\mu(\rho_{AB}^{(p)}) = p.$$

We conclude that entanglement cannot be distilled from $\rho_{AB}^{(p)}$ for $p < 1$ under local operations (but no communication) because for the maximally entangled state we have $\mu(|\psi\rangle\langle\psi|_{AB}) = \mu(\rho_{AB}^{(1)}) = 1$. In fact even common randomness cannot be extracted from these states (under local operations) since for two perfectly correlated bits U, V , we have $\mu(P_{UV}) = 1$. Moreover, having infinitely many copies of $\rho_{AB}^{(p)}$ one cannot locally generate a single copy of $\rho_{AB}^{(q)}$ if $q > p$.

3 More inequalities

In this section we generalize the data processing inequality of the previous section for $\mu(\cdot)$ to other Schmidt coefficients of $\tilde{\rho}_{AB}$. These new inequalities however, do not hold in the n -letter case in the sense of Corollary 3.

Let $1 = \mu_1(\rho_{AB}) \geq \mu_2(\rho_{AB}) \geq \mu_3(\rho_{AB}) \geq \dots$ be Schmidt coefficients of $\tilde{\rho}_{AB}$.

Theorem 4 *Let $\Phi_B : \mathbf{L}(\mathcal{H}_B) \rightarrow \mathbf{L}(\mathcal{H}_{B'})$ be a completely positive trace-preserving super-operator and let $\sigma_{AB'} = \mathcal{I}_A \otimes \Phi_B(\rho_{AB})$. Then for every i we have*

$$\mu_i(\rho_{AB}) \geq \mu_i(\sigma_{AB'}).$$

To prove this theorem it is more convenient to use the isomorphism between the Hilbert spaces $\mathcal{V} \otimes \mathcal{W}$ and $\mathbf{L}(\mathcal{V}, \mathcal{W})$, and the fact that Schmidt coefficients are mapped to singular values under this isomorphism. To be more precise let us fix an orthonormal basis $\{|0\rangle, \dots, |d-1\rangle\}$ for \mathcal{H}_A . Then for every $Z_{AB} \in \mathbf{L}(\mathcal{H}_A) \otimes \mathbf{L}(\mathcal{H}_B)$ there exists a super-operator $\Omega_Z : \mathbf{L}(\mathcal{H}_A) \rightarrow \mathbf{L}(\mathcal{H}_B)$ such that

$$Z_{AB} = \sum_{i,j=0}^{d-1} |i\rangle\langle j|_A \otimes \Omega_Z(|j\rangle\langle i|)_B.$$

Using the fact that $\{|i\rangle\langle j| : i, j = 0, \dots, d-1\}$ is an orthonormal basis for $\mathbf{L}(\mathcal{H}_A)$ it is easy to see that Schmidt coefficients of Z_{AB} are equal to singular values of Ω_Z .

By the above notation we may consider super-operators Ω_ρ and $\Omega_{\tilde{\rho}}$. Observe that

$$\begin{aligned}
\sum_{i,j} |i\rangle\langle j| \otimes \rho_B^{-1/2} \Omega_\rho(\rho_A^{-1/2} |j\rangle\langle i|) &= \sum_{i,j,k} |i\rangle\langle j| \otimes \rho_B^{-1/2} \Omega_\rho(|k\rangle\langle k| \rho_A^{-1/2} |j\rangle\langle i|) \\
&= \sum_{i,j,k} |i\rangle\langle k| \rho_A^{-1/2} |j\rangle\langle j| \otimes \rho_B^{-1/2} \Omega_\rho(|k\rangle\langle i|) \\
&= \sum_{i,k} |i\rangle\langle k| \rho_A^{-1/2} \otimes \rho_B^{-1/2} \Omega_\rho(|k\rangle\langle i|) \\
&= (I_A \otimes \rho_B^{-1/2}) \left(\sum_{i,k} |i\rangle\langle k| \otimes \Omega_\rho(|k\rangle\langle i|) \right) (\rho_A^{-1/2} \otimes I_A) \\
&= (I_A \otimes \rho_B^{-1/2}) \rho_{AB} (\rho_A^{-1/2} \otimes I_A) \\
&= \tilde{\rho}_{AB}.
\end{aligned}$$

Therefore by definition we have

$$\Omega_{\tilde{\rho}}(X) = \rho_B^{-1/2} \Omega_\rho(\rho_A^{-1/2} X). \quad (6)$$

We are now ready to prove Theorem 4.

Proof: From definitions it is clear that $\Omega_\sigma = \Phi \circ \Omega_\rho$, and then from (6) and $\sigma_A = \rho_A$ we have

$$\begin{aligned}
\Omega_{\tilde{\sigma}}(X) &= \sigma_{B'}^{-1/2} \Omega_\sigma(\sigma_A^{-1/2} X) \\
&= \sigma_{B'}^{-1/2} \Phi \left(\Omega_\rho(\rho_A^{-1/2} X) \right) \\
&= \sigma_{B'}^{-1/2} \Phi \left(\rho_B^{1/2} \Omega_{\tilde{\rho}}(X) \right).
\end{aligned}$$

This means that if we define $\Psi : \mathbf{L}(\mathcal{H}_B) \rightarrow \mathbf{L}(\mathcal{H}_{B'})$ by $\Psi(Y) = \sigma_{B'}^{-1/2} \Phi(\rho_B^{1/2} Y)$ then

$$\Omega_{\tilde{\sigma}} = \Psi \circ \Omega_{\tilde{\rho}}.$$

Thus given the correspondence between singular values and Schmidt coefficients we conclude that

$$\mu_i(\sigma_{AB'}) \leq \|\Psi\| \cdot \mu_i(\rho_{AB}),$$

where $\|\Psi\| = \|\Psi\|_\infty$ denotes the operator norm of Ψ , and we use (for example) Problem III.6.2 of [10]. Thus it suffices to show that $\|\Psi\| \leq 1$.

Fix an orthonormal basis $\{|0\rangle, |1\rangle, \dots, |d'-1\rangle\}$ for \mathcal{H}_B and define

$$\tau_{BB'} = \sum_{k,l=0}^{d-1} |k\rangle\langle l| \otimes \Phi \left(\rho_B^{1/2} |k\rangle\langle l| \rho_B^{1/2} \right).$$

It is easy to verify that $\tau_{BB'}$ is a density matrix with marginals $\tau_{B'} = \Phi(\rho_B) = \sigma_B$ and $\tau_B = \rho_B^*$ where by ρ_B^* we mean the entry-wise complex conjugate of ρ_B (with respect to the chosen basis). Moreover we have $\Omega_\tau(X) = \sigma_B^{-1/2} \Phi(\rho_B^{1/2} X^T)$ and then $\Omega_{\tilde{\tau}}(X) = \Psi(X^T)$. As a result $\|\Psi\| = \|\Omega_{\tilde{\tau}}\|$ which we know is equal to the maximum Schmidt coefficient of $\tilde{\tau}_{BB'}$ which is 1. \square

4 Common randomness distillation

In this section we further investigate properties of $\mu(\cdot)$, and address the problem of common randomness distillation under local operations. Let us start with a useful lemma.

Lemma 5 *The optimizers X_A and Y_B in the definition of $\mu(\rho_{AB})$ can be chosen to be hermitian.*

Proof: By restricting the local Hilbert spaces \mathcal{H}_A and \mathcal{H}_B to the supports of ρ_A and ρ_B we may assume that they are invertible. Let $\tilde{\mathbf{L}}_A \subseteq \mathbf{L}(\mathcal{H}_A)$ be the space of operators V such that $\rho_A^{-1/2} V$ is hermitian. Moreover, let $\tilde{\mathbf{L}}_B \subseteq \mathbf{L}(\mathcal{H}_B)$ be the set of operators W such that $W \rho_B^{-1/2}$

is hermitian. Then $\tilde{\mathbf{L}}_A$ and $\tilde{\mathbf{L}}_B$ are subspaces of $\mathbf{L}(\mathcal{H}_A)$ and $\mathbf{L}(\mathcal{H}_B)$, respectively, as *real* vector spaces. Observe that $\tilde{\rho}_{AB}$ is in $\tilde{\mathbf{L}}_A \otimes \tilde{\mathbf{L}}_B$. Thus the vectors in the Schmidt decomposition of $\tilde{\rho}_{AB}$ can be chosen in $\tilde{\mathbf{L}}_A$ and $\tilde{\mathbf{L}}_B$. In fact we may assume that the optimizer $R_A = \rho_A^{1/2} X_A$ and $S_B = Y_B^\dagger \rho_B^{1/2}$ defined in the proof of Theorem 1 belong to $\tilde{\mathbf{L}}_A$ and $\tilde{\mathbf{L}}_B$ respectively. This equivalently means that X_A and Y_B can be chosen to be hermitian. \square

Theorem 6 $0 \leq \mu(\rho_{AB}) \leq 1$ and the followings hold.

- (a) $\mu(\rho_{AB}) = 0$ if and only if $\rho_{AB} = \rho_A \otimes \rho_B$, i.e., ρ_{AB} contains neither classical nor quantum correlation.
- (b) $\mu(\rho_{AB}) = 1$ if and only if there exist local measurements $\{M_A, I_A - M_A\}$ and $\{N_B, I_B - N_B\}$ such that $\text{tr}(\rho_{AB} M_A \otimes N_B) \neq 0, 1$, and

$$\text{tr}(\rho_{AB}(M_A \otimes (I_B - N_B))) = \text{tr}(\rho_{AB}((I_A - M_A) \otimes N_B)) = 0.$$

Proof: $\mu(\rho_{AB}) \geq 0$ is clear from the definition and $\mu(\rho_{AB}) = \lambda_2 \leq \lambda_1 = 1$ follows from the proof of Theorem 1.

(a) $\mu(\rho_{AB}) = 0$ if and only if all Schmidt coefficients of $\tilde{\rho}_{AB}$ except the first one ($\lambda_1 = 1$) are zero, which means that

$$\tilde{\rho}_{AB} = M_1 \otimes N_1 = \rho_A^{1/2} \otimes \rho_B^{1/2},$$

or equivalently $\rho_{AB} = \rho_A \otimes \rho_B$.

(b) Suppose such measurements $\{M_A, I_A - M_A\}$ and $\{N_B, I_B - N_B\}$ exist and let P_{UV} be the bipartite distribution corresponding to the outcomes of these measurements applied to ρ_{AB} . Then by Corollary 3 we have $\mu(\rho_{AB}) \geq \mu(P_{UV})$. On the other hand by assumption binary random variables U and V have perfect correlation, and it is easy to see that $\mu(P_{UV}) = 1$. Thus $\mu(\rho_{AB}) = 1$.

Conversely, suppose $\mu(\rho_{AB}) = 1$, so there exist X_A and Y_B satisfying (2) and (3), and $\text{tr}(\rho_{AB} X_A \otimes Y_B^\dagger) = 1$. By Lemma 5 we can take X_A and Y_B to be hermitian. Moreover, without loss of generality we may assume that ρ_A and ρ_B are invertible.

Define $Z_{AB} = X_A \otimes I_B - I_A \otimes Y_B$. Observe that

$$\begin{aligned} \text{tr}(\rho_{AB} Z Z^\dagger) &= \text{tr}(\rho_{AB} X X^\dagger \otimes I_B) + \text{tr}(\rho_{AB} I_A \otimes Y Y^\dagger) - 2\text{tr}(\rho_{AB} X \otimes Y^\dagger) \\ &= \text{tr}(\rho_A X X^\dagger) + \text{tr}(\rho_B Y Y^\dagger) - 2\text{tr}(\rho_{AB} X \otimes Y^\dagger) \\ &= 0. \end{aligned}$$

Since both ρ_{AB} and $Z Z^\dagger$ are positive semidefinite we conclude that $\rho_{AB} Z Z^\dagger = 0$ and in fact $\rho_{AB} Z = 0$. Equivalently we obtain

$$\rho_{AB}(X_A \otimes I_B) = \rho_{AB}(I_A \otimes Y_B). \quad (7)$$

Observe that

$$\begin{aligned} \rho_{AB}(X_A^2 \otimes I_B) &= \rho_{AB}(X_A \otimes I_B)(X_A \otimes I_B) \\ &= \rho_{AB}(I_A \otimes Y_B)(X_A \otimes I_B) \\ &= \rho_{AB}(X_A \otimes I_B)(I_A \otimes Y_B) \\ &= \rho_{AB}(I_A \otimes Y_B)(I_A \otimes Y_B) \\ &= \rho_{AB}(I_A \otimes Y_B^2). \end{aligned}$$

More generally for every polynomial $q(t)$ we have $\rho_{AB}(q(X_A) \otimes I_B) = \rho_{AB}(I_A \otimes q(Y_B))$.

Using (2), X_A is not a multiple of identity and has a non-trivial eigenspace. On the other hand orthogonal projections on eigenspaces of a hermitian operator can be written as polynomials in terms of that operator with *real* coefficients. Therefore there exists a non-zero orthogonal projection $q(X_A) = M_A \neq I_A$ and a hermitian operator $q(Y_B) = N_B$ such that

$$\rho_{AB}(M_A \otimes I_B) = \rho_{AB}(I_B \otimes N_B).$$

Replacing N_A with N_A^2 , we may assume that N_B is positive semidefinite because

$$\rho_{AB}(I_B \otimes N_A^2) = \rho_{AB}(M_A^2 \otimes I_B) = \rho_{AB}(M_A \otimes I_B).$$

Note that

$$\text{tr}(\rho_B N_B^n) = \text{tr}(\rho_{AB}(I_A \otimes N_B^n)) = \text{tr}(\rho_{AB}(M_A \otimes I_B)) = \text{tr}(\rho_A M_A).$$

Moreover since ρ_A is full-rank and M_A is a non-trivial projection, $0 < \text{tr}(\rho_A M_A) < 1$. Now if N_A has an eigenvalue greater than 1, since ρ_B is full-rank, $\text{tr}(\rho_B N_B^n)$ would tend to infinity as n goes to infinity. We conclude that all eigenvalues of N_B are less than or equal to 1 and $N_B \leq I_B$.

Consider the local measurements $\{M_A, I_A - M_A\}$ and $\{N_B, I_B - N_B\}$ to be applied on ρ_{AB} . The probability of obtaining M_A and $I_B - N_B$ is equal to

$$\begin{aligned} \text{tr}(\rho_{AB}(M_A \otimes (I_B - N_B))) &= \text{tr}(\rho_{AB}(M_A \otimes I_B)) - \text{tr}(\rho_{AB}(M_A \otimes N_B)) \\ &= \text{tr}(\rho_{AB}(M_A \otimes I_B)) - \text{tr}(\rho_{AB}(I_A \otimes N_B)(M_A \otimes I_B)) \\ &= \text{tr}(\rho_{AB}(M_A \otimes I_B)) - \text{tr}(\rho_{AB}(M_A \otimes I_B)(M_A \otimes I_B)) \\ &= \text{tr}(\rho_{AB}(M_A \otimes I_B)) - \text{tr}(\rho_{AB}(M_A \otimes I_B)) \\ &= 0. \end{aligned}$$

Similarly we have $\text{tr}(\rho_{AB}((I_A - M_A) \otimes N_B)) = 0$. We have $\text{tr}(\rho_{AB} M_A \otimes N_B) \neq 0, 1$ because

$$\text{tr}(\rho_{AB} M_A \otimes N_B) = \text{tr}(\rho_{AB} M_A^2 \otimes I_B) = \text{tr}(\rho_A M_A)$$

is strictly between 0 and 1. □

Part (b) of this theorem states that if $\mu(\rho_{AB}) = 1$, then some common randomness can be extracted from ρ_{AB} by local measurements. The converse of this statement also holds; if one bit of common randomness can be extracted from ρ_{AB} , then $\mu(\rho_{AB})$ is at least as large as that of two perfectly correlated bits, which is 1. But what happens if common randomness can be distilled from ρ_{AB} in the sense of asymptotically vanishing probability of error?

To address this question more precisely we start by a definition. We say that C bits of common randomness can be distilled from ρ_{AB} if for every $\epsilon, \delta > 0$ and sufficiently large n there are local measurements on $\rho_{AB}^{\otimes n}$ with outcomes U and V such that

$$\Pr(U \neq V) \leq \epsilon \quad \text{and} \quad H(U) \geq n(C - \delta),$$

where $H(\cdot)$ denotes the entropy function. In the classical case the maximum rate of distillable common randomness is called the Gács-Körner common information and is denoted by $K(A, B)$. It is known that $K(A, B) > 0$ if and only if common randomness can be distilled from ρ_{AB} in the zero-error sense ($\epsilon = 0$) [11, 7]. This implies that for a classical distribution ρ_{AB} , $K(A, B) > 0$ if and only if $\mu(\rho_{AB}) = 1$. This characterization can be generalized to classical-quantum states using the common randomness distillation theorem of [12] and results of [13]. Here we first give a proof that $\mu(\cdot)$ is continuous around the set of perfect correlations and then show that common randomness can be distilled from ρ_{AB} if and only if $\mu(\rho_{AB}) = 1$.

Lemma 7 *Let U, V be two binary random variables such that $p_{01}, p_{10} \leq \epsilon$. Then*

$$\mu(P_{UV}) \geq 1 - \frac{\epsilon}{p_{00}p_{11}} - \frac{2\epsilon^2}{p_{00}p_{11}}.$$

Proof: $\mu(P_{UV})$ is equal to the second singular value of

$$\tilde{P}_{UV} = \begin{pmatrix} \frac{p_{00}}{\sqrt{(p_{00}+p_{01})(p_{00}+p_{10})}} & \frac{p_{01}}{\sqrt{(p_{00}+p_{01})(p_{01}+p_{11})}} \\ \frac{p_{10}}{\sqrt{(p_{10}+p_{11})(p_{00}+p_{10})}} & \frac{p_{11}}{\sqrt{(p_{10}+p_{11})(p_{01}+p_{11})}} \end{pmatrix}.$$

We know that the first singular value of P_{UV} is 1, so the second singular value is equal to

$$\begin{aligned}
\mu(P_{UV}) &= |\det \tilde{P}_{UV}| \\
&= \frac{|p_{00}p_{11} - p_{01}p_{10}|}{\sqrt{(p_{00} + p_{01})(p_{00} + p_{10})(p_{10} + p_{11})(p_{01} + p_{11})}} \\
&\geq \frac{p_{00}p_{11}}{(p_{00} + \epsilon)(p_{11} + \epsilon)} - \frac{p_{01}p_{10}}{p_{00}p_{11}} \\
&\geq 1 - \frac{\epsilon(p_{00} + p_{11}) + \epsilon^2}{p_{00}p_{11}} - \frac{\epsilon^2}{p_{00}p_{11}} \\
&\geq 1 - \frac{\epsilon}{p_{00}p_{11}} - \frac{2\epsilon^2}{p_{00}p_{11}}.
\end{aligned}$$

□

Theorem 8 *Common randomness can be distilled from ρ_{AB} if and only if $\mu(\rho_{AB}) = 1$.*

Proof: If $\mu(\rho_{AB}) = 1$ then by part (b) of Theorem 6 common randomness can be distilled from (even one copy of) ρ_{AB} . Conversely if common randomness can be distilled from ρ_{AB} then by definition for every $\epsilon > 0$ and sufficiently large n , $\rho_{AB}^{\otimes n}$ can be locally transformed to binary random variables U and V such that $\Pr(U \neq V) \leq \epsilon$ and $\Pr(U = V = 0), \Pr(U = V = 1) \geq 1/3$. Thus using Lemma 7 and Corollary 3 we have

$$\mu(\rho_{AB}) \geq 1 - \frac{\epsilon}{q} - \frac{2\epsilon^2}{q},$$

where $q = \Pr(U = V = 0)\Pr(U = V = 1) \geq 1/9$. The claim follows since this inequality holds for all $\epsilon > 0$. □

In the example at the end of Section 2 we see that $\mu(\cdot)$ can indeed take any value between 0 and 1. On pure states however it takes only the extreme values.

Proposition 9 (i) *Suppose ρ_{AB} is pure. Then $\mu(\rho_{AB}) = 0$ if ρ_{AB} is separable and $\mu(\rho_{AB}) = 1$ if ρ_{AB} is entangled.*

(ii) *If $\|\rho_{AB} - \tau_{AB}\|_{\text{tr}} \leq \epsilon$ where τ_{AB} is a maximally entangled state and $\epsilon \leq 1/10$, then $\mu(\rho_{AB}) \geq 1 - 9\epsilon$.*

Proof: (i) If ρ_{AB} is separable, $\mu(\rho_{AB}) = 0$ follows from part (a) of Theorem 6. Thus suppose $\rho_{AB} = |\psi\rangle\langle\psi|_{AB}$ where $|\psi\rangle_{AB}$ is entangled with Schmidt decomposition

$$|\psi\rangle_{AB} = \sum_i \alpha_i |v_i\rangle_A \otimes |w_i\rangle_B.$$

Since $|\psi\rangle_{AB}$ is entangled at least two of the Schmidt coefficients (say) α_1 and α_2 are non-zero. Define

$$X_A = c\alpha_2^2 |v_1\rangle\langle v_1| - c\alpha_1^2 |v_2\rangle\langle v_2|,$$

and

$$Y_A = c\alpha_2^2 |w_1\rangle\langle w_1| - c\alpha_1^2 |w_2\rangle\langle w_2|,$$

where $c^{-1} = \alpha_1\alpha_2(\alpha_1^2 + \alpha_2^2)^{1/2}$. Then X_A and Y_B satisfy (2), (3) and $\text{tr}(\rho_{AB}X_A \otimes Y_B) = 1$. As a result $\mu(\rho_{AB}) = 1$.

(ii) Since τ_{AB} is a maximally entangled state, there are local measurements $\{M_A^0, M_A^1\}$ and $\{N_B^0, N_B^1\}$ such that $\text{tr}(\tau_{AB}M_A^0 \otimes N_B^1) = \text{tr}(\tau_{AB}M_A^1 \otimes N_B^0) = 0$ and

$$\text{tr}(\tau_{AB}M_A^0 \otimes N_B^0) = \frac{1}{d} \left\lfloor \frac{d}{2} \right\rfloor, \quad \text{tr}(\tau_{AB}M_A^1 \otimes N_B^1) = \frac{1}{d} \left\lceil \frac{d}{2} \right\rceil,$$

where d is the minimum of the dimensions of registers A and B . Let

$$p_{uv} = \text{tr}(\rho_{AB}M_A^u \otimes N_B^v).$$

Then using $\|\rho_{AB} - \tau_{AB}\|_{\text{tr}} \leq \epsilon$ we find that

$$\left| p_{00} - \frac{1}{d} \left\lfloor \frac{d}{2} \right\rfloor \right| + \left| p_{11} - \frac{1}{d} \left\lceil \frac{d}{2} \right\rceil \right| + p_{01} + p_{10} \leq \epsilon,$$

which using $\epsilon \leq 1/10$ implies

$$p_{00}p_{11} \geq \left(\frac{1}{d} \left\lfloor \frac{d}{2} \right\rfloor - \epsilon \right) \left(\frac{1}{d} \left\lceil \frac{d}{2} \right\rceil - \epsilon \right) \geq \left(\frac{1}{3} - \epsilon \right) \left(\frac{2}{3} - \epsilon \right) \geq \frac{7 \times 17}{30^2}, \quad (8)$$

and $p_{01} + p_{10} < \epsilon$. By Corollary 3 we have $\mu(\rho_{AB}) \geq \mu(P_{UV})$. So it suffices to show that $\mu(P_{UV}) \geq 1 - 9\epsilon$ which is a simple consequence of Lemma 7. \square

Although part (ii) of this proposition states the continuity of $\mu(\cdot)$ at maximally entangled states, by part (i) it takes values 0 or 1 on pure states and is not continuous at separable states. Here we argue that such a seemingly undesirable property is unavoidable. That is, assuming the two properties of $\mu(\cdot)$ stated in Theorem 2, which are the main motivations of this work, and continuity around maximally entangled states (part (ii) of the above proposition), we show that $\mu(|\psi\rangle\langle\psi|_{AB}) = 1$ for every entangled pure state. The main point is that every entangled pure state $|\psi\rangle_{AB}$ is distillable under local trace non-increasing maps. More precisely, by considering local projections onto typical subspaces we find that for every $\epsilon, \delta > 0$, there exist n and completely positive trace non-increasing super-operators Φ and Ψ such that

$$\sigma_{EF} = (1 + \delta)\Phi \otimes \Psi(|\psi\rangle\langle\psi|_{AB}^{\otimes n}),$$

is a normalized state and ϵ -close (in trace distance) to a maximally entangled state. Thus using Theorem 2 we have

$$(1 + \delta)^{1/2} \mu(|\psi\rangle\langle\psi|_{AB}) \geq \mu(\sigma_{EF}),$$

Now considering the continuity of $\mu(\cdot)$ at maximally entangled states and taking the limit $\epsilon, \delta \rightarrow 0$, we conclude that $\mu(|\psi\rangle\langle\psi|_{AB}) = 1$.

5 Concluding remarks

We introduced a measure of correlation $\mu(\rho_{AB})$ with the property that $\mu(\rho_{AB}^{\otimes n}) = \mu(\rho_{AB})$, and proved a data processing inequality for this measure. We showed that this measure fully characterizes quantum states from which common randomness can be distilled.

$\mu(\cdot)$ is a measure of total classical and quantum correlations and takes its maximum value on two perfectly correlated bits. This implies that $\mu(\cdot)$ is not well-behaved under (even one bit of) classical communication. It is tempting to look for a measure of *quantum* correlation with the above properties that vanishes on classically correlated states. In that case we could use such a measure to study the problem of entanglement distillation under LOCC maps. Even proving the nonexistence of such a measure would be interesting.

Acknowledgements. The author is thankful to Amin Gohari for introducing [1], and to Yury Polyanskiy for sending a copy of his related works. This research was in part supported by a grant from IPM (No. 91810409).

References

- [1] Wei Kang and Sennur Ulukus, A New Data Processing Inequality and Its Applications in Distributed Source and Channel Coding, IEEE Transactions on Information Theory **57**, 56–69 (2011)
- [2] S. Kamath and V. Anantharam, Non-interactive Simulation of Joint Distributions: The Hirschfeld-Gebelein-Rényi Maximal Correlation and the Hypercontractivity Ribbon, Proceedings of the 50th Annual Allerton Conference on Communications, Control and Computing (2012).

- [3] H. O. Hirschfeld, A connection between correlation and contingency, *Proc. Cambridge Philosophical Soc.* **31**, 520-524 (1935).
- [4] H. Gebelein, Das statistische problem der Korrelation als variations-und Eigenwertproblem und sein Zusammenhang mit der Ausgleichungsrechnung, *Z. für angewandte Math. und Mech.* **21**, 364–379 (1941).
- [5] A. Rényi, New version of the probabilistic generalization of the large sieve, *Acta Math. Hung.* **10**, 217-226 (1959).
- [6] A. Rényi, On measures of dependence, *Acta Math. Hung.* **10**, 441-451 (1959).
- [7] H. S. Witsenhausen, On sequences of pairs of dependent random variables, *SIAM Journal on Applied Mathematics*, 28: 100-113 (1975).
- [8] Y. Polyanskiy, Hypothesis testing via a comparator, *Information Theory Proceedings (ISIT)*, 2012 IEEE International Symposium on, 2206-2210 (2012).
- [9] Gowtham Kumar, Binary Rényi Correlation, http://www.stanford.edu/~gowthamr/research/binary_re (December 2012).
- [10] R. Bhatia, *Matrix Analysis*, Springer (2010).
- [11] P. Gács and J. Körner, Common information is far less than mutual information. *Problems of Control and Information Theory*, 2(2):119–162, 1972
- [12] Igor Devetak and Andreas Winter, Distilling common randomness from bipartite quantum states, *IEEE Transactions on Information Theory* **50**, 3183–3196 (2004).
- [13] P. Hayden, R. Jozsa, D. Petz, and A. Winter, Structure of states which satisfy strong subadditivity of quantum entropy with equality, *Communications in Mathematical Physics*, 246(2): 359–374, 2004.